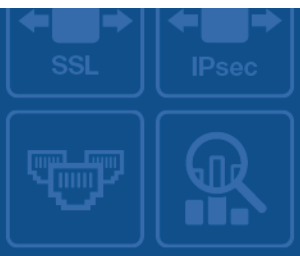
FORTINET
High Performance Network Security

Managing a FortiSwitch unit with a FortiGate

for FortiOS 5.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Monday, April 24, 2017

Managing a FortiSwitch unit with a FortiGate

for FortiOS 5.4

TABLE OF CONTENTS

Change Log

Date	Change Description
June 8, 2016	Initial release for FortiOS 5.4.1
June 14, 2016	Minor corrections.
June 17, 2016	Added additional port CLI commands to the **FortiSwitch Port Features** chapter.
July 6, 2016	Added a note that you must enable fortilink-split-interface for a FortiLink aggregate interface that connects to more than one switch.
Sept 30, 2016	Clarified that a FortiLink Split-Interface must contain exactly two physical ports (one for each FortiSwitch).
Oct 20, 2016	Added list of FortiGate models that do not support FortiLink in FOS 5.4.1.
April 24, 2017	Corrected the CLI syntax in Creating VLANs on page 29.

Introduction

The maximum number of supported FortiSwitches depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitches Supported
Up to FortiGate-98 and FortiGate-VM01	8
FortiGate-00 to 280 and FortiGate-VM02	24
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-000 and up	128
FortiGate-3*xxx* and up, and FortiGate-VM08 and up	256

Supported Models

The following table shows the FortiSwitch models that support Fortilink mode when paired with the corresponding FortiGate models and the listed minimum software releases.

FortiGate Models	Earliest FortiOS	FortiSwitch Models
FGT-90D	5.2.2	FS-224D-POE
FGT-60D FGT-90D FGT-100D, FGT-140D (POE, T1) FGT-200D, FGT-240D, FGT-280D (POE) FGT-600C FGT-800C FGT-1000C	5.2.3	FSR-112D-POE FS-108D-POE FS-124D FS-124D-POE FS-224D-POE FS-224D-FPOE
	5.4.0	All FortiSwitch D-series models. FortiSwitchOS 3.3.x or 3.4.0 is recommended.

FortiGate Models	Earliest FortiOS	FortiSwitch Models
FGT-1200D FGT-1500D FGT-3700D FGT-3700DX	5.4.0	All FortiSwitch D-series models. FortiSwitchOS 3.3.x or 3.4.0 is recommended.
All FortiGate models that support FortiOS 5.4.1, with the following exceptions: FGR-30D, FGR-30D-A FGR-35D FG-52E FWF-60E FG-61E , FWF-61E FG-2000E FG-2500E	5.4.1	All FortiSwitch D-series models. FortiSwitchOS 3.4.2 or later is required in all managed switches.
FGT_60E FGT_61E FWF_60E FWF_61E FGT_100E FGT_101E	5.4.2	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required in all managed switches.
FGT_80E, FGT_80E_POE FGT_81E, FGT_81E_POE FGT_100EF	5.4.3	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required in all managed switches.

What's New

The following new Fortilink features are available

FortiOS 5.4.1 with FortiSwitchOS 3.4.2 (or later release)

- FortiLink support added for all of the FortiGate models
- Supports FortiSwitch stacking topologies
- Syslog Export from FortiSwitch to FortiGate
- Visibility in the FortiGate of devices connected to FortiSwitch ports
- FortiGate CLI support for FortiSwitch features (on non-FortiLink ports):
  - Spanning Tree
  - Link Aggregation Groups
  - Storm Control

- Trusted/Untrusted Ports support (for DHCP snooping)
- Port Statistics Display

Before You Begin

Before you configure the managed FortiSwitch unit, the following assumptions have been made in the writing of this manual:

- You have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch, and you have administrative access to the FortiSwitch web-based manager and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate web-based manager and CLI.

How this Guide is Organized

This guide contains the following sections:

- Connecting FortiLink Ports - information about connecting FortiSwitch ports to FortiGate ports.
- FortiLink Configuration Using FortiGate GUI
- FortiLink Configuration Using FortiGate CLI
- Configuring Fortilink for FortiGate HA - how to configure Fortilink for FortiGate units in HA mode.
- Network Topologies for Managed FortiSwitch - describes configuration for various stacking topologies
- Optional Setup Tasks - describes other set up tasks.
- VLAN Configuration - configure VLANs from the FortiGate unit.
- FortiSwitch Port Features - configure Ports and POE from the FortiGate unit. Add STP and LAG?
- Additional Capabilities - describes additional FortiLink features in 5.4.1
- Troubleshooting - describes techniques for troubleshooting common problems.

Connecting FortiLink Ports

This section contains information about the FortiSwitch and FortiGate ports that you connect to establish a FortiLink connection.

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit.

In FortiSwitchOS 3.3.0 and later releases, you can use any of the switch ports for FortiLink. Some or all of the switch ports (depending on the model) support auto-discovery of the FortiLink ports.

You have a choice of connecting a single FortiLink port or multiple FortiLink ports as a logical interface (link-aggregation group, hardware switch or software switch).

Summary of the Steps

1. If required,enable the Switch Controller on FortiGate
2. Connect a cable between the FortiSwitch port(s) and the FortiGate port(s)

Enable the Switch Controller on FortiGate

Prior to connecting the FortiSwitch and FortiGate units, ensure that the Switch Controller feature is enabled on the FortiGate (depending on the FortiGate model and software release, this feature may be enabled by default).

Use the FortiGate web-based manager or CLI to enable the Switch Controller.

Using the FortiGate web-based manager

1. Go to **System > Feature Select**.
2. Turn on the **Switch Controller** feature.
3. Select **Apply**.

The menu option **WiFi & Switch Controller** now appears in the web-based manager.

Using the FortiGate CLI

Use the following command to enable the Switch Controller.

```
config system global
   set switch-controller enable
end
```

Connect the FortiSwitch and FortiGate

In FortiSwitchOS 3.3.0 and later releases, FortiSwitchOS provides additional flexibility for FortiLink:

- Use any switch port for FortiLink
- Provides auto-discovery of the FortiLink ports on the FortiSwitch
- Choice of a single FortiLink port or multiple FortiLink ports in a link-aggregation group (LAG)

Auto-discovery of the FortiSwitch Ports

In releases FortiSwitchOS 3.3.0 and beyond, the D-series FortiSwitch models support FortiLink auto-discovery, which is automatic detection of the port connected to the FortiGate.

You can use any of the switch ports for FortiLink. Use the following FortiSwitch CLI commands to configure a port for FortiLink auto-discovery:

```
config switch interface
   edit <port>
   set auto-discovery-fortilink enable
end
```

NOTE: Some FortiSwitch ports are enabled for auto-discovery by default. See table below.

NOTE: Complete this configuration step BEFORE connecting the switch to the FortiGate.

Each FortiSwitch model provides a set of ports that are enabled for FortiLink auto-discovery by default. If you connect the FortiLink using one of these ports, no switch configuration is required.

In general (in FortiSwitchOS 3.4.0 and later releases), the last four ports are the default auto-discovery FortiLink ports. You can also run the **show switch interface** CLI command on the FortiSwitch to see the ports that have auto-discovery enabled.

The table below lists the default auto-discovery ports for each switch model:

FortiSwitch Model	Default Auto-FortiLink ports
FS-108D	ports 9 and 10
FSR-112D	ports 9, 10, 11 and 12
FS-124D, FS-124D-POE	ports 23, 24, 25 and 26
FS-224D-POE	ports 21, 22, 23 and 24
FS-224D-FPOE	ports 25, 26, 27 and 28
FS-248D-POE	ports 49, 50, 51, and 52
FS-248D-FPOE	ports 49, 50, 51, and 52
FS-424D, FS-424D-POE, FS-424D-FPOE	ports 25 and 26
FS-448D, FS-448D-POE, FS-448D-FPOE	ports 49, 50, 51, and 52
FS-524D, FS-524D-FPOE	ports 25, 26, 27, 28, 29 and 30

FortiSwitch Model	Default Auto-FortiLink ports
FS-548D, FS-548D-FPOE	ports 49, 50, 51, 52, 53 and 54
FS-1024D, FS-1048D, FS-3032D	all ports

Choosing the FortiGate Ports

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit. The FortiGate manages all of the switches through one active FortiLink. The FortiLink may consist of one port or multiple ports (for a LAG).

As a general rule, FortiLink is supported on all ports that are listed as LAN ports or Switch ports.

FortiLink Configuration Using FortiGate GUI

This section describes the configuration steps to establish a FortiLink between a FortiSwitch and a FortiGate unit.

You can configure FortiLink using the FortiGate web-based manager (GUI) or the FortiGate CLI. We recommend using the FortiGate GUI, because the CLI steps are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection (single port or LAG) with zero configuration steps on the FortiSwitch, and with a few simple configuration steps on the FortiGate.

Summary of the Steps

1. On the FortiGate, configure the FortLink port or create a logical FortLink interface.
2. Authorize the managed FortiSwitch.

Configure FortiLink as a Single Link

Configure the FortiLink port on the FortiGate using the following steps:

1. Go to **Network** > **Interfaces**
2. (Optional) If the FortiLink physical port is currently included in the internal interface, edit the internal interface and remove the desired port from the Physical Interface Members.
3. Edit the FortiLink port.
4. Enter the following fields in the **Edit Interface** form:
    a. **Addressing mode**: Set to **Dedicated to FortiSwitch**.
    b. **IP/Network Mask**: system automatically sets the IP address and network mask.
    c. (Optional) **Automatically authorize devices**: disable to manually authorize the FortiSwitch.
    d. Click **OK**.

Configure FortiLink as a Logical Interface

You can configure the FortiLink as a logical interface: link-aggregation group (LAG), hardware switch or software switch).

NOTE: LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above. Hardware switch is supported on some FortiGate models.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch. Make sure that you configure auto-discovery on the FortiSwitch ports (unless the port is a default auto-discovery port).

1. Go to **Network> Interfaces**
2. (Optional) If the FortiLink physical ports are currently included in the internal interface, edit the internal interface and remove the desired ports from the Physical Interface Members.

3. Click **Create New**
4. Enter the following fields in the **Add Interface** form:
   a. **Interface name**: enter a name for the interface (11 characters maximum).
   b. **Type**: select **802.3ad Aggregate**, **Hardware Switch**, or **Software Switch**.
   c. **Physical Interface Members** : select the FortiGate ports for the logical interface.
   d. **Addressing mode**: set to **Dedicated to FortiSwitch**.
   e. **IP/Network Mask**: system automatically sets the IP address and network mask.
   f. (Optional) **Automatically authorize devices**: disable to manually authorize the FortiSwitch.
   g. Click **OK**.

FortiLink Split-Interface

You can create a FortiLink Split-Interface, which connects a FortiLink aggregate interface from one FortiGate to two FortiSwitches.

NOTE: The aggregate interface for this configuration must contain exactly two physical ports (one for each FortiSwitch).

You must enable the Split-Interface option on the FortiLink aggregate interface. From the FortiGate CLI, enter the following commands:

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface enable
end
```

Authorizing the FortiSwitch

If you configured the FortiLink interface to manually authorize the FortiSwitch as a managed switch, perform the following steps:

1. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
2. (Optional)Click on the FortiSwitch faceplate and click **Authorize**. This step is required only if you disabled the automatic authorization field of the interface.

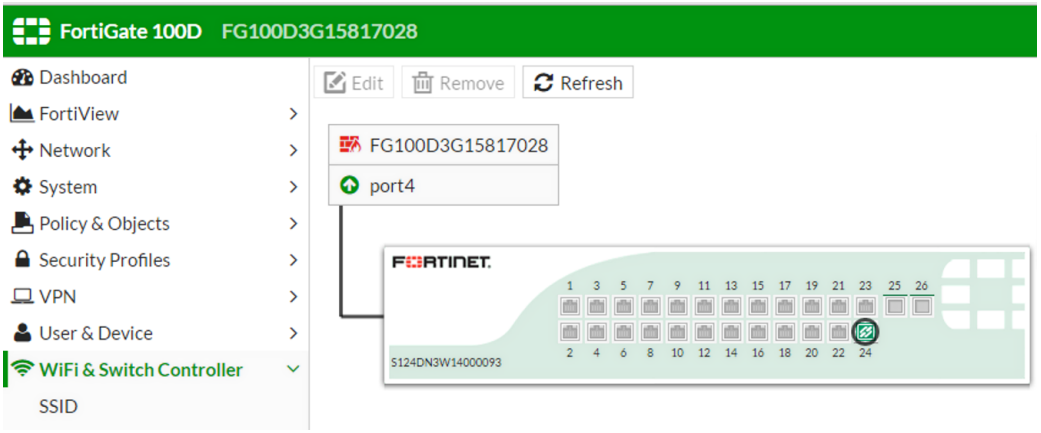
Managed FortiSwitch Display

The Managed FortiSwitch page displays the FortiGate name and its FortiLink interface, and the faceplate for the connected switch.

When the FortiLink is established successfully, the status is green (next to the FortiGate interface name and on the FortiSwitch faceplate) and the link between the ports is a solid line.

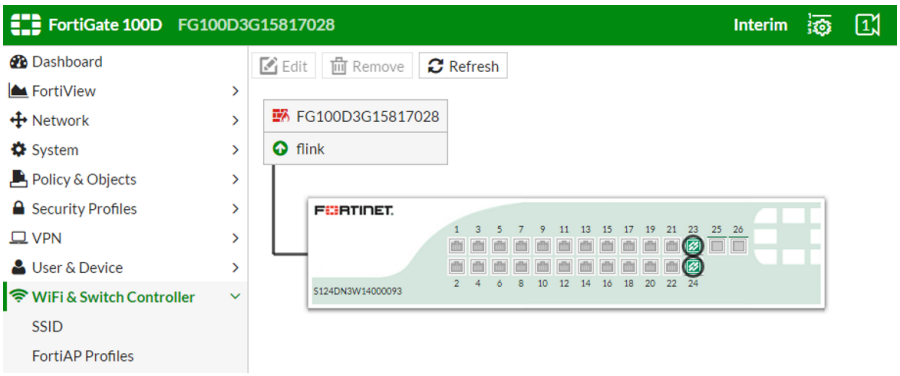
FortiLink as Single Link

The page displays the FortiLink port number on the FortiGate and the FortiLink port is highlighted in green on the FortiSwitch faceplate.



FortiLink as Logical Interface

The page displays the FortiLink interface name on the FortiGate and the FortiLink ports are highlighted in green on the FortiSwitch faceplate.



Edit Managed FortiSwitch

To edit the managed FortiSwitch, perform the following steps:

1. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
2. Click on the FortiSwitch faceplate and click **Edit**.
3. In the **Edit Managed FortiSwitch** form, you can input a name and a description for this switch.
4. Click **OK** to save the changes.

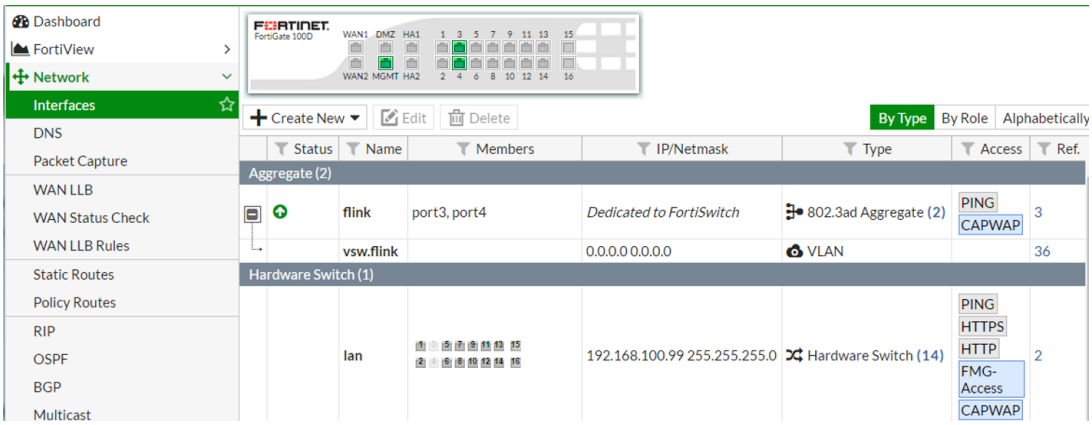
From the **Edit Managed FortiSwitch** form, you can also perform the following actions:

- Click **Restart** to restart the FortiSwitch.
- Click **De-authorize** to stop the FortiSwitch from being managed by this FortiGate.
- Click **Upgrade** to upgrade the switch. The system will prompt you for the new image file to upload and install.

Network Interface Display

In **System** > **Network** > **Interfaces**, the system displays the interface type, and displays **Dedicated to FortiSwitch** in the IP/Netmask field.

The following figure shows the Interfaces table entry for a FortiLink LAG. The table also displays the VLANs associated with the interface.



FortiLink Configuration Using FortiGate CLI

This section describes how to configure FortiLink using the FortiGate CLI. We recommend using the FortiGate GUI, because the CLI steps are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection (single port or LAG) with zero configuration steps on the FortiSwitch, and with a few simple configuration steps on the FortiGate.

Summary of the Steps

1. Remove the port(s) from the LAN interface.
2. Configure the FortLink port or create a logical FortLink interface.
3. Configure NTP.
4. Authorize the managed FortiSwitch.
5. Configure DHPC

Configure FortiLink as a Single Link

Configure the FortiLink port on the FortiGate, and authorize the FortiSwitch as a managed switch.

In the following steps, port1 is configured as the FortiLink port.

1. If required, remove port 1 from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port1
      end
   end
end
```

2. Configure for port 1 as the FortiLink interface

```
config system interface
   edit port1
      set auto-auth-extension-device enable
      set fortilink enable
   end
end
```

3. Configure an NTP server on port 1.

```
config system ntp
   set server-mode enable
   set interface port1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

```
    config switch-controller managed-switch
       edit FS224D3W14000370
          set fsw-wan1-admin enable
       end
    end
NOTE: FortiSwitch will reboot when you issue the above command.
```

Configure FortiLink as a Logical Interface

You can configure the FortiLink as a logical interface: link-aggregation group (LAG), hardware switch or software switch).

NOTE: LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above. Hardware switch is supported on some FortiGate models.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch. Make sure that you configure auto-discovery on the FortiSwitch ports (unless the port is a default auto-discovery port).

In the following steps, port4 and port5 are configured as a FortiLink LAG.

1. If required, remove the FortiLink ports from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port4
         delete port5
      end
   end
end
```

2. Create a trunk with the two ports that you connected to the switch:

```
config system interface
   edit flink1 (enter a name, 11 characters maximum)
      set allowaccess ping capwap https
      set vlanforward enable
      set type aggregate
      set member port4 port5
      set lacp-mode static
      set fortilink enable
      (optional) set fortilink-split-interface enable
   next
end
```

NOTE: you must enable **fortilink-split-interface** if the members of the aggregate interface connect to more than one FortiSwitch.

3. Configure an NTP server on the LAG interface:

```
config system ntp
   set server-mode enable
   set interface flink1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
```

NOTE: FortiSwitch will reboot when you issue the above command.

5. Configure a DHCP server on port 1.

```
config system dhcp server
   edit 0
      set ntp-service local
      set default-gateway 169.254.254.1
      set netmask 255.255.255.252
      set interface flink1
      config ip-range
         edit 1
            set start-ip 169.254.254.2
            set end-ip 169.254.254.2
         end
      set vci-match enable
      set vci-string FortiAP FortiSwitch FortiExtender
   end
end
```

Configuring FortiLink for FortiGate HA

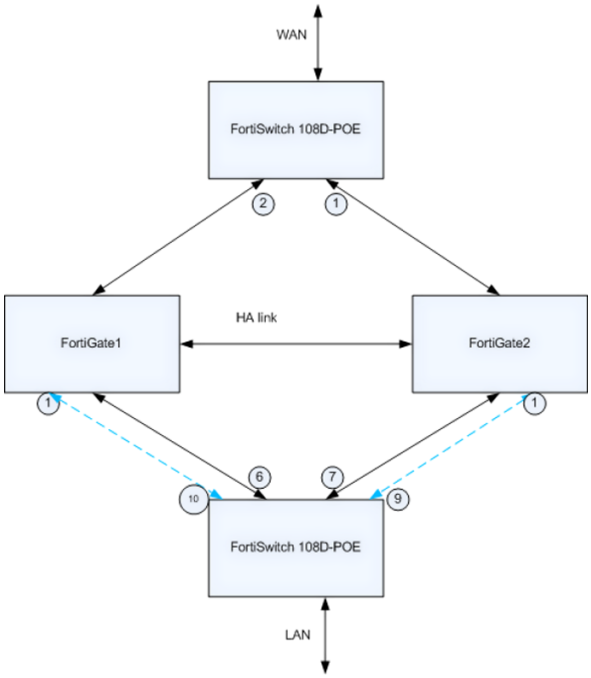
With FortiOS 5.4.0 and later releases, a FortiGate operating in HA mode can use FortiLink (to FortiSwitches running FortiSwitchOS 3.3.0 or later release).

To use FortiLink mode with a pair of FortiGate units in a high-availability cluster, you must connect FortiLink from the switch to both of the FortiGate units.

Highlights of this configuration:

1. No console port or direct management is required on the FortiSwitch.
2. All the actions described here can be performed from FortiCloud if needed
3. All FortiSwitch internal state and counters are visible when in FortiLink managed mode

Example Topology



The LAN and WAN links connect to FortiSwitch ports. The FortiSwitch connects to the active and standby FortiGate units. If the standby FortiGate (for example, FGT2) becomes active, this is transparent to the LAN and WAN ports. FortiLink is automatically established to FGT2, and the active traffic path becomes LAN <-> FGT2<-> WAN.

Note the following points:

1. FortiSwitch connects with FortiLink to both of the FortiGate units.
2. LAN and WAN links can connect to separate FortiSwitches, as shown in the figure. You can also connect them to the same FortiSwitch (and use VLANs to separate the LAN and WAN traffic).

3. Connect the FortiLinks from any two FortiSwitch ports to FGT1 port X and FGT2 port X, where the FortiGate port numbers must match (port1 in the above topology diagram).
4. For a Logical FortiLink interface with two ports, connect Fortilinks from two additional FortiSwitch ports to FGT1 port Y and FGT2 port Y, where the FortiGate port numbers must match.

Adding a Second FortiGate to Existing Single FortiGate

Connect an additional FortiLink from the FortiSwitch to the new FortiGate, and configure HA on both of the FortiGate units.

Configuration Steps

Configuration consists of the following major steps:

1. Configure “auto-discovery-fortilink enable” on the FortiSwitch ports that you will connect to FGT2. This step is not required if the port is auto-fortilink by default.
2. Add cable connections from FGT2 to the directly-connected FortiSwitches (exact duplicate of FGT1 to the FortiSwitches)
3. Connect HA cables between FGT1 and FGT2
4. At FGT1: configure FortiGate High Availability using the GUI. For additional information, refer to the High Availability chapter in the FortiOS Handbook.
5. At FGT2: Configure FortiGate High Availability using the CLI from the console port. The following parameters must be identical to FGT1:
   - HA-mode
   - Priority
   - Group Name and Password
6. At this point, the FGT1 synchronizes with FGT2. This takes several minutes.
7. Verify the configuration at FGT2 using the following commands:

```
get ha status
get system ha status
```

Adding the First Switch to Existing HA FortiGates (single FortiLinks)

Connect one FortiSwitch port to each of the FortiGate units. On FGT1, follow the same FortiLink configuration steps as for the non-HA configuration. FGT1 synchronizes the configuration with FGT2.

Configuration Steps

1. Configure two FortiSwitch ports as “auto-discovery-fortilink enable”. This step is not required for any port is auto-fortilink by default.
2. Connect one port to FGT1 and the other port to FGT2.
   - The FGT1 and FGT2 port numbers must be identical For example:
   - FortiSwitch port21 and port22 connect to FGT1 port4 and FGT2 port4

3. At FGT1, perform the steps to configure FortiLink (as described in FortiLink Configuration Using FortiGate GUI):
   a. Configure a port to be the FortiLink port
   b. Authorize the FortiSwitch
4. At FGT2, run the command "get switch-controller managed-switch" to verify that the FGT1 configuration was synchronized successfully

Adding the First Switch to Existing FGT HA setup (Logical Fortilink Interface)

In this configuration, connect two FortiSwitch ports to each FortiGate unit. Enter the configuration commands on FGT1 (same commands as for the non-HA configuration). The HA feature synchronizes the configuration to FGT2.

Configuration Steps

1. Configure four FortiSwitch ports as “auto-discovery-fortilink enable”. This step is not required for any port is auto-fortilink by default.
2. Connect two ports to FGT1 and the other ports to FGT2
   - the FGT1 and FGT2 port numbers must be the same. For example:
   - FortiSwitch port21 and port22 connect to FGT1 port4 and port5 and FortiSwitch port23 and port24 connect to FGT2 port4 and port5
3. At FGT1, configure the Fortilink interface (as described in FortiLink Configuration Using FortiGate GUI):
   a. Create the FortiLink logical interface and add the physical ports as members
   b. Authorize the FortiSwitch
4. At FGT2, run command "get switch-controller managed-switch" to verify that the FGT1 configuration was synchronized successfully

(Optional) Test the HA Capability

Warning: the following is a destructive test that simulates a FortiGate failure. You should conduct this test only in a lab or test network, not in a production network:

1. Disconnect power from FGT1 to simulate failure
2. From the FGT2 UI:
   Check **Wifi and Switch Controller** > **Managed FortiSwitch**
3. FortiSwitch is now visible from the management interface on FGT2

Network Topologies for Managed FortiSwitch

With releases prior to FortiOS 5.4.1, the FortiGate required a separate FortiLink for each managed FortiSwitch. Starting in release FortiOS 5.4.1, the FortiGate requires only one active FortiLink to manage all of the subtending FortiSwitches. We refer to this new capability as "Stacking".

You can configure the FortiLink as a physical interface or as a logical interface (associated with one or more physical interfaces). Depending on the network topology, you may also configure a standby FortiLink.

For any of the topologies, note the following:

- All of the managed FortiSwitches will function as one Layer-2 stack. The FortiGate manages each FortiSwitch separately.
- The active FortiLink carries data as well as management traffic.

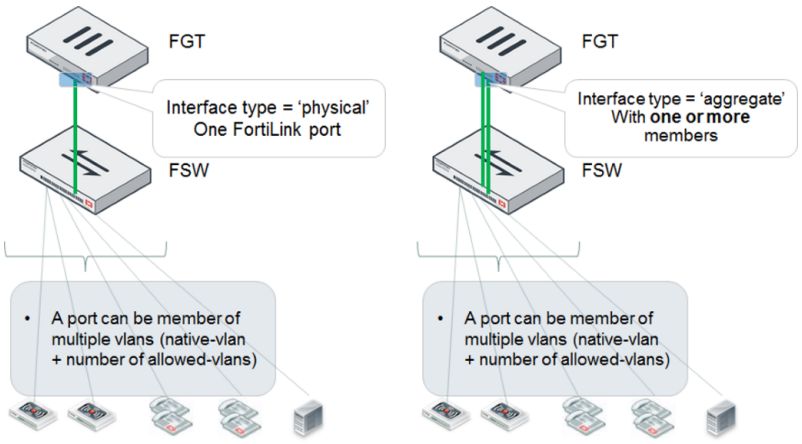
Supported Topologies

Fortinet recommends the following topologies for managed FortiSwitches:

- Single FortiGate managing a single FortiSwitch
- Single FortiGate managing a stack of several FortiSwitches
- HA-mode FortiGate managing a single FortiSwitch
- HA-mode FortiGate managing a stack of several FortiSwitches
- HA-mode FortiGate managing a FortiSwitch two-tier topology
- Single FortiGate managing multiple FortiSwitches (using hardware or software switch interface)
- Enterprise/Office Closet Topology

Single FortiGate managing a single FortiSwitch

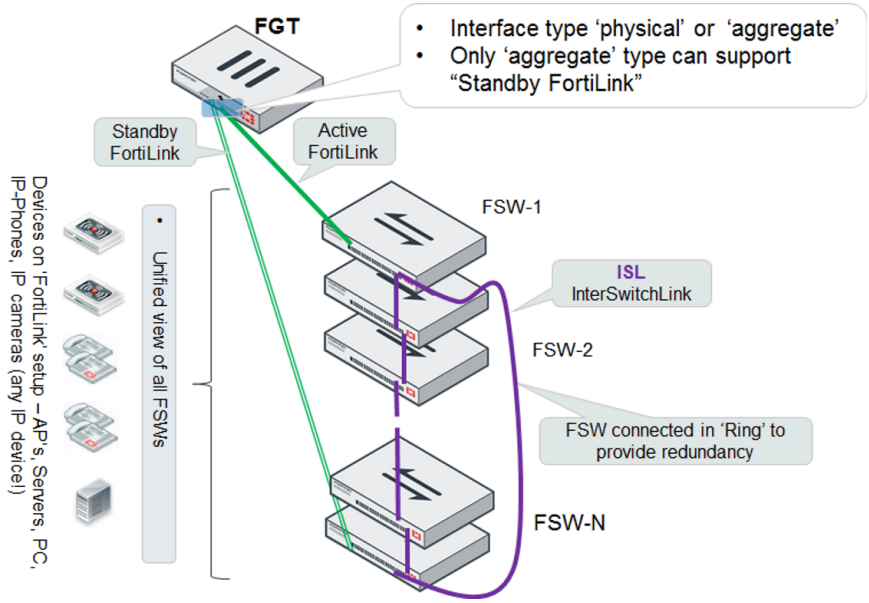
On the FortiGate, the FortiLink interface is configured as physical or aggregate. The 802.3ad aggregate interface type provides a logical grouping of one or more physical interfaces.



Single FortiGate managing a stack of several FortiSwitches

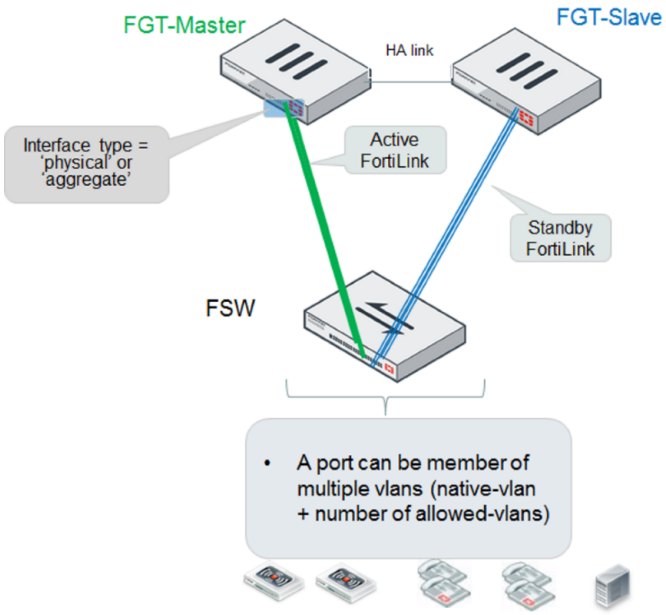
The FortiGate connects directly to one FortiSwitch device using a physical or aggregate interface. The remaining FortiSwitches connect in a ring using inter-switch links.

Optionally, you can connect a standby FortiLink connection to the last FortiSwitch. For this configuration, you create a FortiLink Split-Interface (an aggregate interface which contains one active link and one standby link).



HA-mode FortiGate managing a single FortiSwitch

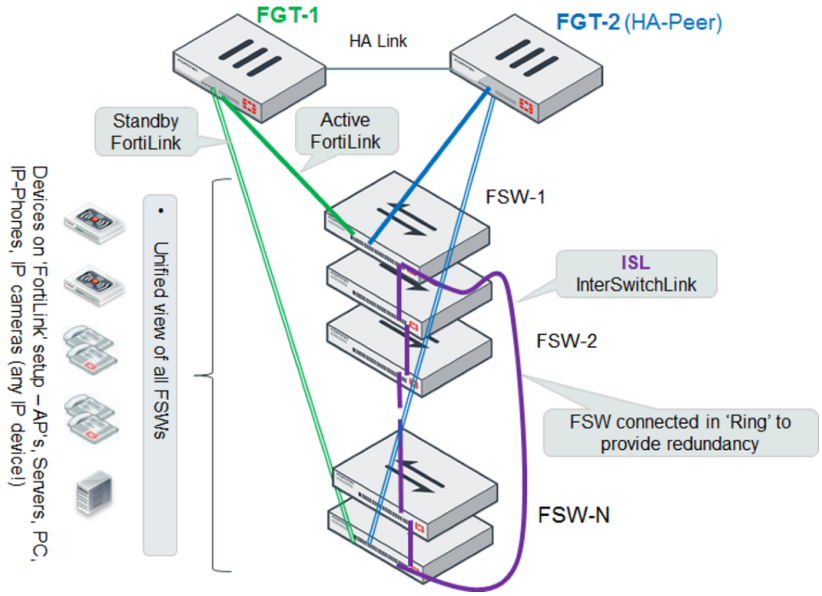
The master and slave FortiGate units both connect a FortiLink to the FortiSwitch. The FortiLink port(s) and interface type must match on the two FortiGate units.



HA-mode FortiGate managing a stack of several FortiSwitches

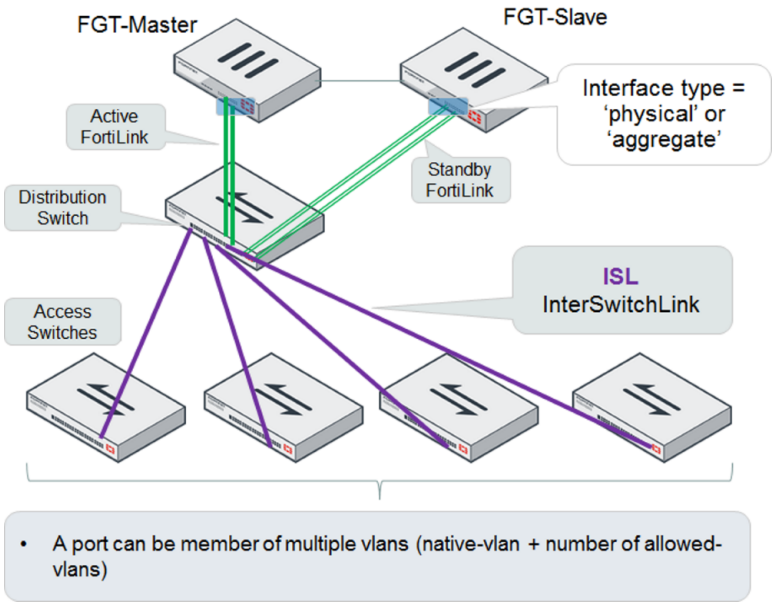
The master and slave FortiGate units both connect a FortiLink to the first FortiSwitch, and (optionally) to the last FortiSwitch. The FortiLink ports and interface type must match on the two FortiGate units.

For the active/standby FortiLink configuration, you create a FortiLink Split-Interface (an aggregate interface which contains one active link and one standby link).



HA-mode FortiGate managing a FortiSwitch two-tier topology

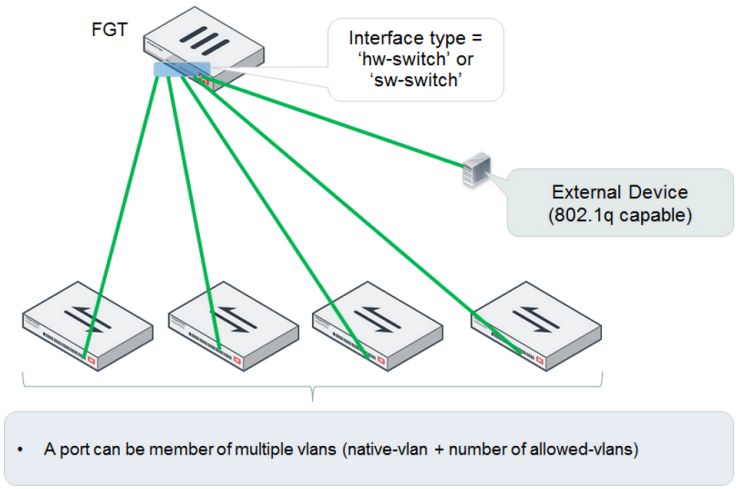
The distribution FortiSwitch connects to the master and slave FortiGate units. The FortiLink port(s) and interface type must match on the two FortiGate units.



Single FortiGate managing multiple FortiSwitches (using hardware or software switch interface)

The FortiGate connects directly to each FortiSwitch. Each of these FortiLink ports is added to the logical hardware-switch or software-switch interface on the FortiGate.

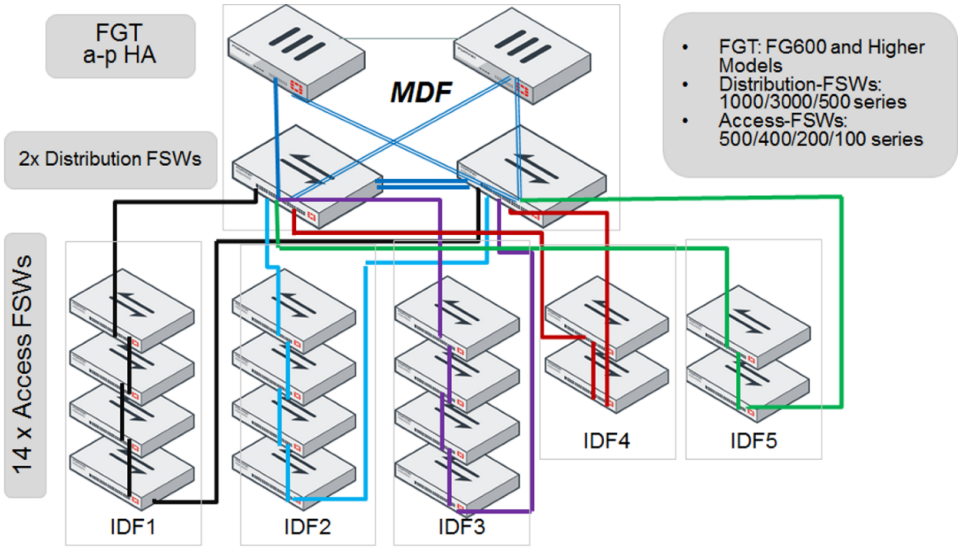
Optionally, you can connect other devices to the FortiGate logical interface. These devices will have Layer 2 connectivity with the FortiSwitch ports. The device must support IEEE 802.1q VLAN tagging.



Enterprise/Office Closet Topology

HA-mode FortiGates connect to redundant distribution FortiSwitches. Access FortiSwitches are arranged in a stack in each IDF, connected to both distribution switches.

For the FortiLink connection to each distribution switch, you create a FortiLink Split-Interface (an aggregate interface which contains one active link and one standby link).



Stacking Configuration

The configuration steps for stacking include:

1. Configure the active FortiLink interface on the FortiGate.
2. (Optional) Configure the standby FortiLink interface.
3. Connect the FortiSwitches together, based on your chosen topology.

1. Configure the Active FortiLink

Configure the FortiLink interface (as described in the FortiLink Configuration section).

When you configure the FortiLink interface, stacking capability is enabled automatically.

2. Configure the Standby FortiLink

Configure the standby FortiLink interface. Depending on your configuration, the standby FortiLink may connect to the same FortiGate as the active Fortilink, or to a different FortiGate.

If the FortiGate receives discovery requests from two FortiSwitches, the link from one FortiSwitch will be selected as active and the link from other FortiSwitch will be selected as standby.

If the active FortiLink fails, FortiGate converts the standby FortiLink to active.

3. Connect the FortiSwitches

Refer to the topology diagrams to see how to connect the FortiSwitches.

Inter-switch links (ISLs) form automatically between the stacked switches.

FortiGate will discover and authorize all of the FortiSwitches that are connected. After this, the FortiGate is ready to manage all of the authorized FortiSwitches.

Disable Stacking

To disable stacking, execute the following command from the FortiGate CLI. In the following example, port4 is the FortiLink interface:

```
config system interface
   edit port4
      set fortilink-stacking disable
   end
end
```

Optional Setup Tasks

This section describes the following tasks:

- Configuring FortiSwitch Management Port
- Converting to FortiSwitch Standalone Mode

Configuring FortiSwitch Management Port

If the FortiSwitch model has a dedicated management port, you can configure remote management to the FortiSwitch. In FortiLink mode, the FortiGate is the default gateway, so you need to configure an explicit route for the FortiSwitch management port.

Using the FortiSwitch Web-based Manager

1. Go to **Routing**
2. Under **Static Routes**, click **Create New**
3. Enter the following fields in the **New Static Route** form:
   a. Destination: enter a subnetwork and mask
   b. Device: select the management interface
   c. Gateway: enter the gateway IP address

Using the FortiSwitch CLI

Enter the following commands:

```
config router static
   edit 1
      set device mgmt
      set gateway <router IP address>
      set dst <router subnet> <subnet mask>
   end
end
```

In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
      set dst 192.168.0.0 255.255.0.0
   end
end
```

Converting to FortiSwitch Standalone Mode

If a FortiSwitch is operating in managed mode, follow these instructions to convert it to standalone mode.

1. From the switch CLI:

```
config system global
   set mgmt-mode local
end
NOTE: FortiSwitch will reboot when you issue the above command.
```

2. From the FortiGate, use the web-based manager or CLI to perform the following commands before the switch reboot has completed:

Using the Web-based manager

a. Navigate to **WiFi & Switch Controller** > **Managed FortiSwitch**.

b. Right-click on the switch and select **De-authorize**.

Using the CLI

```
config switch-controller managed-switch
   edit <switch-id>
      set fsw-wan1-admin disable
   end
end
```

VLAN Configuration

Use Virtual Local Area Networks (VLANs) to logically separate a LAN into smaller broadcast domains. VLANs allow you to define different policies for different types of users and to set finer control on the LAN traffic (traffic is only sent automatically within the VLAN. You must configure routing for traffic between VLANs).

From the FortiGate, you can centrally configure and manage VLANs for the managed FortiSwitches.

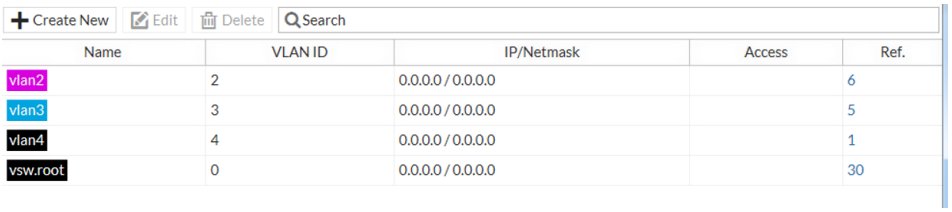
In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch supports untagged and tagged frames in Fortilink mode. The switch supports up to 1023 user-defined VLANs. The user can assign a VLAN number (in the range 1-4095) to each of the VLANs.

You can configure the default VLAN for each FortiSwitch port. You can also configure a set of allowed VLANs for each FortiSwitch port.

FortiSwitch VLANs Display

The **WiFi & Switch Controller** > **FortiSwitch VLANs** page displays VLAN information for the managed switches.

The following figure shows the VLAN page:



Each entry in the VLAN list displays the following information:

- **Name** - name of the VLAN
- **VLAN ID** - the VLAN number.
- **IP/Netmask** - Address and mask of the subnetwork that corresponds to this VLAN
- **Access**
- **Ref** - how many interfaces reference this VLAN.

Creating VLANs

Setting up a VLAN requires:

- Creating the VLAN.
- Assigning FortiSwitch ports to the VLAN.

Using the web-based manager

Creating the VLAN

1. Go to **WiFi & Switch Controller** > **FortiSwitch VLANs** and select **Create New**. Change the following settings:

Interface Name	VLAN name
VLAN ID	Enter a number (1-4094)
Color	Choose a unique color for each VLAN, for ease of visual display.
IP/Network Mask	IP address and network mask for this VLAN.

1. Enable **DHCP Server**. Set the IP range.
2. Set the **Admission Control** options as required.
3. Select **OK**.

Assigning FortiSwitch Ports to the VLAN

1. Go to **WiFi & Switch Controller** > **FortiSwitch Ports**.
2. Click the rows for ports to select them.
3. To change the native VLAN, click the **Native VLAN** column in one of the selected entries.
4. Select a VLAN from the displayed list. The new value is assigned to the selected ports.
5. To change the allowed VLANs, click the **+** icon in the **Allowed VLANs** column.
6. Select one or more of the VLANs from the displayed list. You can also select the value **all**. The new value is assigned to the selected port.

Using the CLI

1. Create the marketing VLAN.

```
config system interface
   edit <vlan name>
      set vlanid <1-4094>
      set color <1-32>
      set interface <fortilink-enabled-interface>
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit <vlan name>
      set ip <IP address> <Network mask>
end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway <IP address>
      set dns-service default
      set interface <vlan name>
```

```
            config ip-range
               set start-ip <IP address>
               set end-ip <IP address>
            end
         set netmask <Network mask>
   end
```

4. Assign ports to the VLAN.

```
   config switch-controller managed-switch
      edit <Switch ID>
         config ports
            edit <port name>
               set vlan <vlan name>
               set allowed-vlans <vlan name>
               or
               set allowed-vlans-all enable
            next
         end
   end
```

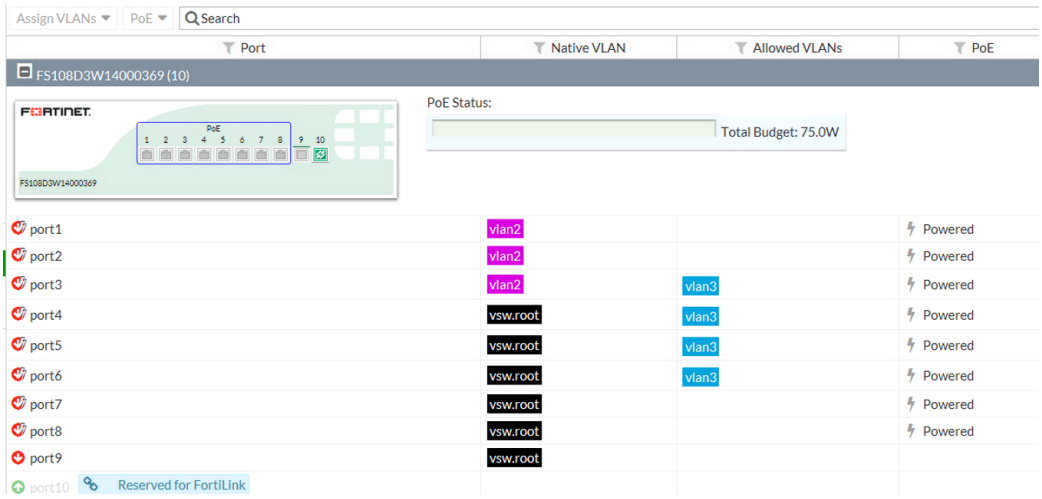
FortiSwitch Port Features

You can configure the FortiSwitch port feature settings from the FortiGate using the FortiGate web-based manager or CLI commands.

FortiSwitch Ports Display

The **WiFi & Switch Controller** > **FortiSwitch Ports** page displays port information about each of the managed switches.

The following figure shows the display for a FortiSwitch 108D-POE:

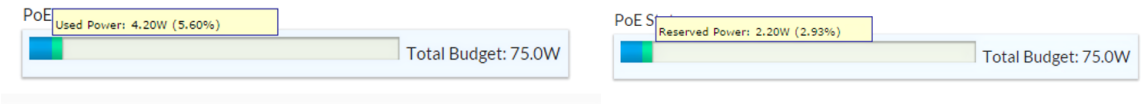


The switch faceplate displays:

- the active ports (green)
- the POE-enabled ports (blue rectangle)
- the FortiLink port (link icon)

The POE Status displays the total power budget, and the actual power currently allocated.

The allocated power displays a blue bar for the used power (currently being consumed) and a green bar for the reserved power (power available for additional devices on the POE ports). See the following figures:



Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- Native VLAN
- Allowed VLANs
- POE status

Configuring Ports Using the Web Manager

You can use the web manager to configure VLANs on the port (see VLAN Configuration), or to enable/disable POE on a port.

Enable or Disable POE on a port

Follow these instructions to configure POE on a port:

1. Navigate to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click on a row to select the port.
3. Right-click the row, select **POE** and select **Enable POE** or **Disable POE**

Note: when you select a row in the port table, you can also use the **Assign VLANs** and **PoE** menus (located just below the page banner), instead of the right-click menu, to configure the values.

Configuring Ports Using the FortiGate CLI

You can configure the following FortiSwitch port settings using the FortiGate CLI:

- Set port speed and admin status
- Configure vlan on the port (see VLAN Configuration)
- DHCP trust setting
- Enable or disable POE

Configuring Port Speed and Admin Status

Use the following commands to set port speed and other basis port settings:

```
config switch-controller managed-switch
   edit <switch>
      config ports
         edit <port>
            set description <text>
            set speed <speed>
            set status {down | up}
```

Configuring DHCP Snooping

Set the port as a trusted or untrusted DHCP-snooping interface:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set dhcp-snooping {trusted | untrusted}
```

Configuring POE

The following POE CLI commands are available starting in FortiSwitchOS 3.3.0:

Enable PoE on the Port

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set poe-status {enable | disable}
```

Reset the POE port

The following command resets POE on the port

```
execute switch-controller poe-reset <fortiswitch-id> <port>
```

Display general POE status

```
get switch-controller <fortiswitch-id> <port>
```

The following example displays the POE status for port 6 on the specified switch:

```
# get switch-controller poe FS108D3W14000967 port6
Port(6) Power:3.90W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 78mA
```

Configuring STP

Starting in FortiSwitch release 3.4.2, STP is enabled by default for the non-FortiLink ports on the managed FortiSwitches. Use the following commands to enable or disable STP on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-state (enabled | disabled)
```

Additional Capabilities

FortiOS 5.4.1 introduces additional capabilities related to managed FortiSwitch.

FortiSwitch LOG export

You can enable/disable the managed FortiSwitches to export their syslogs to the FortiGate. The setting is global, and the default setting is disabled.

The FortiGate sets the user field to "fortiswitch-syslog" for each entry, to allow a level of filtering.

CLI Command Syntax:

```
config switch-controller switch-log
   status (enable | disable)
   severity [ emergency | alert | critical | error | warning | notification | *information
       | debug ]
end
```

You can override the global log settings for a FortiSwitch, using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config switch-log
         set local-override enable
```

At this point, you can configure the log settings that apply to this specific switch.

FortiSwitch Per-Port Device Visibility

In the FGT GUI, **User & Device** > **Device LIst** displays a list of devices attached to the FortiSwitch ports. For each device, the table displays the IP address of the device, and the interface (FortiSwitch name and port).

From the CLI, the following command displays information about the host devices:

```
diagnose switch-controller dump mac-hosts_switch-ports
```

FortiGate CLI support for FortiSwitch features (on non-FortiLink ports)

```
You can configure the following FortiSwitch features from the FortiGate CLI.
```

Configuring LAG

You can configure a link aggregation group for non-fortilink ports on a FortiSwitch. You cannot configure ports from different FortiSwitches in one LAG.

```
config switch-controller managed-switch
```

```
   edit <switch-id>
      config ports
         edit <trunk name>
            set type trunk
            set mode < static | lacp > Link Aggreation mode
            set bundle (enable | disable)
            set min-bundle <int>
            set max-bundle <int>
            set members < port1 port2 ...>
         next
      end
   end
end
```

Configuring Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. Storm control uses the data rate of the link to measure traffic activity.

When the data rate exceeds the configured threshold, storm control drops excess traffic. You can configure the types of traffic to drop: broadcast, unknown unicast, or multicast.

The Rate units is packets per second. The default value is 500.

The Storm Control settings are global to all of the non-FortiLink ports on the managed switches. Use the following CLI commands to configure storm control:

```
config switch-controller storm-control
   set rate <rate>
   set unknown-unicast (enable | disable)
   set unknown-multicast (enable | disable)
   set broadcast (enable | disable)
end
```

You can override the global Storm Control settings for a FortiSwitch, using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config storm-control
         set local-override enable
```

At this point, you can configure the Storm Control settings that apply to this specific switch.

Display Port Statistics

Port stats will be accessed via FSW REST Monitor API.

Execute Custom FortiSwitch Commands

From the FortiGate, you can execute FortiSwitch commands on the managed FortiSwitch.

This feature adds a simple scripting mechanism for users to configure generic commands to be executed on the switch.

Create a command

Use the following syntax to create a command file:

```
config switch-controller custom-command
   edit <cmd-name>
      set command " <FortiSwitch commands>"
```

The following example creates a command file to set the STP max-age parameter:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting
         set max-age 10
         end
      "
   next
end
```

Execute a command

After you have created a command file, use the following command on the FortiGate to execute the command file on the target switch:

```
exec switch-controller custom-command <cmd-name> <target-switch>
```

The following example runs command **stp-age-10** on the specified target FortiSwitch:

```
FGT30E3U15003273 # exec switch-controller custom-command stp-age-10 S124DP3X15000118
```

Troubleshooting

If the FortiGate does not establish the Fortilink connection with the switch, perform the following troubleshooting checks.

Troubleshooting FortiLink Issues

Check the FortiGate configuration

Using the FortiGate GUI, check the FortiLink interface configuration:

1. In **Network** > **Interfaces**, double-click the interface used for FortiLink.
2. Ensure that **Dedicated to Extension Device** is set for this interface.

Using the FortiGate CLI, Verify that you have configured the DHCP and NTP settings correctly. Enter the following commands:

1. Verify that the NTP server is enabled, and the Fortilink interface has been added to the list:

```
show system ntp
```

2. Ensure that the DHCP server on the Fortilink interface is configured correctly:

```
show system dhcp
```

Check the FortiSwitch configuration

Use the following FortiSwitch CLI commands to check the FortiSwitch configuration:

1. Verify that the switch system time matches the time on the FortiGate:

```
get system status
```

2. Verify that FortiGate has sent an IP address to the FortiSwitch.
Typically, the IP address will be in the range of 169.254.x.x:

```
get system interfaces
```

3. Verify that you can ping the FortiGate IP address:

```
exec ping x.x.x.x
```